SECURITY - PHYSICAL AND DATA CHAPTER 14

(FILE NAME ON DISK # 1 = S2C14.WPD)

One of the most important assets of an organization is information. As such, protecting or securing information and facilities that process and maintain information is vital to operations. The impact of security deficiencies are lost business, damaged reputations, fiduciary losses, lost assets, and possibly lost trade secrets. Security controls are needed to safeguard information from unauthorized or accidental modification, destruction, and disclosure, and to ensure timeliness, availability and usability of data. Possible threats to operations include ignorance and carelessness, fire and water damage, disgruntled or unethical employees, outsiders or hackers, and viruses.

The organization needs a comprehensive written security plan to minimize exposure to all threats and risks. This program should emphasize the need for asset protection, security, and controls. The degree of control should be based on an assessment of risk in relation to the value of the asset. It also should reflect proper concerns for the sensitivity of information. Three major areas that must be reviewed to ensure that IS operations and information are not vulnerable to undue risks and exposures are: physical security; data security; and backup and contingency planning. This chapter focuses on the first two risk areas. Corporate contingency planning is discussed in Chapter 10.

SECURITY ADMINISTRATION AND ACCOUNTABILITY

Management must regulate and monitor the computer environment by establishing security standards, policies, procedures, and controls that are incorporated into the organization's normal business practices. Maintaining a secure environment requires ongoing vigilance. After establishing a security plan, security procedures should be developed to ensure the plan's provisions are followed, and threats to the system are quickly detected. Responsibility for security should reside with the security administrator and/or information security personnel. The security administrator or information security personnel must be familiar with the organization's overall security policies and should have the authority to recommend and implement controls in strategic areas. They also should, if acting as LAN administrator, be thoroughly familiar with the LAN's administration. Personnel departments should be responsible for tracking all terminations and providing notification to the appropriate security personnel. Depending on the size of the organization, security measures can range from simple file scanning to full-scale surveillance of equipment and data files. Such measures also may include issuing user identification codes, maintaining and establishing user security levels, and controlling access to sensitive data and program files. In general, security administration responsibilities should include:

- Performing risk analysis.
- Establishing, enforcing and monitoring the security program for all platforms (mainframe, minicomputer, LANs, and PCs).
- Acting as a liaison between users and management.
- Reviewing user access codes periodically for appropriate access levels.

Personnel assigned security administration duties also should not be involved with input authorization and preparation, computer operations, programming, or output reconciliation duties. Proper segregation of security functions is not always possible in institutions with limited staff. In those cases where segregation of duties is impractical, management should ensure an appropriate independent review of security administration activities is conducted by a knowledgeable third party. In smaller institutions this independent review may be conducted by a non-involved manager or senior officer.

Security administration for a PC may be different than that on a mainframe, minicomputer, or LAN. Mainframe and LAN administration is centralized

through the use of security software. PC software is implemented and administered on each individual unit. Because computers are widely distributed throughout the financial institution, the administrator may need to delegate immediate supervision to designated persons within user areas or assign a departmental security contact who is responsible for overseeing and coordinating the area's security requirements and controls. These individuals in turn would report security violations to the security administrator.

SECURITY PLAN

An overall security plan includes: physical protection of the data facility and IS equipment throughout the organization and data security. The plan should be developed with the approval and involvement of top management and the board of directors and cover all functions performed in the IS operation and all areas touched by automation. Senior management's commitment to security should be emphasized and provisions for communicating security objectives to all employees should be clearly specified.

Security of the IS operation must be integrated with the security plan of the entire organization. Capable senior officials should be charged with its development, implementation, and administration. Generally, their responsibilities fall into two areas: the design of security techniques, and procedures for day-to-day security operations. Extensive security measures will be ineffective if not properly implemented. Therefore, active employee participation and enforcement at all levels is vital. A well-developed security training program that includes regular a review of security procedures will reduce the vulnerability of the organization. Properly trained IS auditors can independently assess the extent to which a formal security plan is being followed and may play a key role in assuring its adequacy.

The first element of the plan is concerned with physical protection of the data processing facility and all computer equipment. It should include measures to minimize exposure or the probability of threat to all computer hardware and software throughout the organization. Computer resources within the institution should be ranked in order of importance and protected with a commensurate level of security. Identification of the protection provided, the significance of specific threats, and individuals responsible for execution of the program should be specified in the plan. Using technical and administrative precautions, together with operational and procedural controls, will help reduce the probability of accidents. A description of electronic or mechanical devices selected to prevent and detect physical threats also should be included. Management may want to restrict access to this sensitive information so that protection measures are not compromised. The security program also must consider proper insurance provisions as detailed in Chapter 9.

The second element of the security plan should include proper preventative and detective measures to reduce the risk of interruption of business due to unauthorized access and manipulation of data and programs, and inaccurate or incomplete processing. The accuracy and integrity of data is depends on proper control procedures for processing in both the user and data processing areas of the institution.

USER EDUCATION

Users have varying levels of expertise and familiarity with computers. A user education program should be implemented to promote awareness regarding the use and care of computers and their obligation to challenge any person or procedure that may violate security systems. Users should have operation and procedural manuals available for reference. Training sessions should be held during equipment installation. Additionally, training should be included as part of new employees' orientation whose duties involve using computers. Suggested topics for training sessions include:

- Corporate policy regarding the use of computers.
- Data security policies and procedures and their implementation.
- User involvement and responsibility toward promoting data security.
- Disciplinary action taken when data security policies are violated.

PHYSICAL, BUILDING, CABINET, AND VAULT SECURITY

An uninterrupted IS operation depends upon provisions to prevent, detect, minimize, and recover losses from damage or unauthorized use of equipment, software, or data. Protective measures against intentional and accidental threats should be included in these physical security measures.

A physical security plan should be designed to obtain maximum protection at a reasonable cost. Although it may not be practical to completely safeguard a computer installation, thorough evaluation of alternatives is important. This evaluation should include a risk assessment that consists of determining what needs to be secured (e.g., information, equipment, personnel, network services such as E-mail, applications, software, etc.), sources of risks (e.g., environmental occurrences, viruses, hackers, and unethical employees), probability of occurrence, costs and remedies available to minimize exposure.

Physical security must be coordinated with the entire data processing operation and not regarded as an independent function. Controls and procedures, such as backup, housekeeping, auditing, and documentation, supplement the protection provided by physical security measures. It may be difficult to quantify or assess the success of physical security efforts. However, with proper management support and employee training, the overall effectiveness of all IS operations is enhanced through such safeguards.

Building Security

When selecting a site for a computer facility, management's major objective is to limit the risk of environmental exposure from internal and external sources. The selection process should include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Outside intruders can be deterred through the use of guards, fences, barriers, surveillance equipment, or other similar devices. Since access to the data center should be limited, doors and windows must be secured.

Some intruder detection devices available include:

- Switches that activate an alarm when an electrical circuit is broken.
- Light and laser beams, ultraviolet beams and sound or vibration detectors that are invisible to the intruder.
- Ultrasonic and radar devices that detect movement in a room.
- Closed-circuit television.

The detection devices should provide continuous coverage. Security guards should be properly instructed about their duties. The data center employees who access secured areas should have proper identification, such as badges. All visitors should sign-in and wear proper IDs so that they can be identified easily. Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. Security guards should be educated as to who is permitted to remove assets from the premises and record the identity of anyone removing them. Consideration should be given to implementing a specific and formal authorization process for the removal of PCs from the premises.

Actual building security precautions will vary depending on size and location of the data center and/or institution. If the center is located in a separate building, extensive security precautions may be appropriate for the entrances and perimeter. If the institution is housed in an office building, security precautions should focus on entry from other areas of the building. Many computer centers use magnetic encoded key cards to unlock doors. In many cases these systems are managed by a PC and will maintain a daily access activity log the time of day access was provided. Key cards may be selectively encoded to allow a proof operator, for instance, to gain entry to the computer center but not to the computer room. The cards also may be encoded for specific time-of-day entry to further their control. In addition, extra precautions should be taken to physically secure cabling when floor space of a building is utilized by the organization versus a separate building. It would be much easier to tap the wiring in a building that is shared by other tenants rather than a building in which the institution is the sole occupant.

Cabinet and Vault Security

Protective containers are designed to meet either fire-resistant or burglar-resistant standards. Labels describing expected tolerance levels are usually attached to safes and vault doors.

PHYSICAL SECURITY FOR PCS AND DISTRIBUTED IS ENVIRONMENTS

A computer located in a user department is often less secure than one located in a computer room. Minicomputers or other distributed data processing environments (e.g., Local Area Networks or LANs) that offer a full range of applications for small financial institutions as well as larger organizations are commonly housed throughout the organization, without special environmental controls or raised flooring. In such situations, physical security precautions are often less sophisticated than those found in large data centers, and overall building security becomes more important. All computers, however, should be physically separate from other financial institution operations and internal control procedures should be established regardless of the size of the computer. The level of security surrounding any computer should depend on the significance of the applications processed and risks to the organization, the cost of equipment, and the availability of backup equipment.

Because of their portability, PCs often are prime targets for theft and misuse. The location of PCs determines the extent of physical security required. PCs located in unrestricted facilities should, at a minimum, be protected by a physical barrier – such as a counter or divider – preventing easy access by customers. Employees also should have restricted access to PCs and data. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls.

An advantage of PCs is that they can operate in an office environment. This provides flexible and informal processing operations. However, as with larger systems, PCs are sensitive to environmental factors such as smoke, dust, heat, humidity, food particles, and liquids. Because they are not usually located within a protected data processing center, housekeeping practices should be adapted to provide protection from ordinary contaminants.

Other environmental problems to guard against include electrical power surges and static electricity. The electrical power supply in an office environment is sufficient for a PC's requirements. However, periodic fluctuations in power (surges) can cause equipment damage or loss of data. PCs in carpeted areas are susceptible to static electrical discharges that can cause damage to PC components or memory.

Physical security for distributed data processing, particularly LANs, which are usually PC-based, is slightly different than for mainframe or minicomputer platforms. With a network there is often no centralized computer room. In addition, a network often extends beyond the local premises. There are certain components which need physical security. These include the hardware devices and the software and data that may be stored on the file servers, PCs, or removable media (tapes and disks). As with the traditional mainframe or minicomputer environment, physical network security should prevent unauthorized personnel from accessing LAN devices or the transmission of data.

Physical protection for networks as well as PCs includes: power protection, physical locks, security guards, magnetic badge readers, secure dial-up modems, diskless workstations, data encryption, and backups. Physical access to the network servers (files, applications, communications, etc.) should be off limits to anyone but the LAN administrator. Network workstations or PCs should be password protected and monitored for all workstation activity. Network wiring requires some form of protection since it does not have to be physically penetrated for the data it carries to be revealed. Network security also can be compromised by capturing radio frequency emissions.

PERSONNEL, DATA FILE MEDIA, AND COMPUTER OPERATIONS SECURITY

Personnel security is vital to the overall security plan. The quality of the data processing function and organization is directly related to the quality of its personnel. Most computer systems are vulnerable to staff tampering. Implementing security controls over personnel and assigning responsibility for monitoring and enforcing these procedures play a major role in

establishing a sound operation. In addition, adequate security over computer operations can yield secondary benefits, such as error-rate reductions, improved quality, better scheduling, and more timely results.

Written operating procedures should be current and sufficiently detailed to guide the organization and operation of the computer center. Access to the computer room must be restricted to authorized personnel. The best environment is created when only the computer operations personnel (operators and supervisors) are allowed in the computer room.

Computer operators should be denied access to program flowcharts, source decks, program listings, etc., since they are not required to perform programming duties. These items should be secured and maintained outside the computer room to prevent unauthorized changes to programs by computer operators.

Programmers, input/output control clerks, systems analysts, consultant engineers, etc., should be restricted from entering the computer room. All work should be delivered and picked up through dispatch windows or a scheduling department. If an authorized visitor requires admittance to the computer room, regular check-in and check-out control procedures should be followed. The physical layout of some computer facilities may not permit complete restriction, particularly if the tape/disk library is located within the confines of the computer room. The computer room should be locked at all times and exits should be readily accessible from the inside.

The tape/disk file library should be protected from physical disaster in the same manner as the computer room. In addition, the library should be controlled throughout all operating shifts to prevent unauthorized access to data file media. During shifts in which a librarian is not present, alternate procedures may be implemented. All media within the library, such as magnetic tapes, disk packs and cards should be stored in a closed, dust-free, fire-resistant area. Removal of these files from the library should be permitted only when needed for processing. In addition, all critical data and software on the various media should be backed up and stored off-site. This provides an easy recovery should a crisis occurs.

Control of sensitive forms is another important security concern. Printed forms of a negotiable nature (checks, stock certificates, etc.) and signature plates are vulnerable to misapplication and must be secured. Appropriate controls include dual control locks for forms within a secure location and inventory records that specify date, time of access, and personnel accessing the secure location. The supply of forms should be issued according to scheduled production runs. Periodic inventories should be completed for all forms. Any checks that are voided during processing should be distributed to appropriate users for accountability.

The physical security plan also should address the personnel and data media protection for the equipment, data, and software necessary to operate the PC and local area networks. All LAN-based servers should be located in a secured room. Access to the servers should be limited to LAN administrators and other computer operators if necessary. It is unlikely that the physical access to standalone PCs can be secured. If the PC cannot be housed in a secured area, such as behind a locked door or in a locked drawer, a key entry system or software security must be in place to prevent unauthorized users from accessing the unit.

Storage devices for PCs and LANs (such as hard disks, diskettes, and tape media) can be damaged by excessive heat, smoke, dust, liquids, and other contaminants. Diskettes, the most common medium of storage, are more sensitive and require more care than hard disks and tapes. It is important that all personnel learn to handle diskettes properly. All data media should be externally labeled to identify contents and avoid mishandling. Diskettes and tapes should be stored in a physically secure location when not in use. Backup and off-site storage is necessary for key data to ensure proper recovery.

HARDWARE AND SOFTWARE INVENTORY

The inventory system should record all hardware, including terminals, servers, PC equipment and peripherals. This includes their purchase, distribution and disposal. A hardware inventory should include:

- Manufacturer's name and model number.
- Identifying serial number.

- Cost.
- Date of purchase.
- Current location.
- Name of user or user group responsible for use.

A hardware inventory system should facilitate resource sharing, software distribution and maintenance, and repair or replacement of equipment. To ensure proper record keeping and compatibility with other hardware and software in use, ordering and distribution of hardware should be centralized under the authority of the information systems department. All security administrators should receive a copy of the most recent inventory listing.

Software Inventory

All software, whether purchased or developed in house, should be accounted for through an inventory system. Additionally, vendor contracts for purchased software should be centrally maintained. Inventory maintenance is important because it:

- Facilitates locating software for replacements or upgrades.
- Can be used to identify what software is executed at a particular PC and the person(s) accountable.
- Reduces risks of violating software licensing agreements (for purchased software only).
- Provides internal controls for institutional assets.

The inventory listing should include the following information:

For purchased software:

- Date of purchase.
- Product and manufacturers' names.
- Identify whether purchased outright or under a licensing agreement.
- Cost.
- Version number.
- Serial number.
- User area where installed.
- Number of copies installed for use on the server.

For in-house developed software:

- Program name.
- Program developer.
- Initial date of creation.
- Date last updated.
- User area where installed.

The individual responsible for all software acquisitions and maintenance should have an up-to-date copy of the inventory listing. This individual also should be aware of contract terms, such as copyright restrictions and maintenance responsibilities.

Copyright Protections

Purchased software is usually licensed for use rather than purchased outright. Such proprietary software is protected by copyright. The license specifies how many copies the financial institution is entitled to and may identify which machine(s) and how many users may use the software. Violations of the licensing agreement expose the institution to possible costly litigation. In addition, illegally installed software may ultimately lead to operational inefficiencies. For example, effective maintenance would be difficult to implement since unauthorized copies of software would not be recorded in an inventory system. This may result in unauthorized users utilizing obsolete versions.

Caution should be taken when purchasing network software. Many software programs are not licensed for shared use on a network. Individual copies must be purchased for each network user. There are software packages that can be acquired for a network that allow only a predetermined number of persons to utilize the programs concurrently rather than acquiring a licensed copy for each individual user on the network. For example, instead of purchasing a licensing agreement for 100 specific users who are defined to the network, an organization may acquire a 50 concurrent usage site license since no more than 50 individuals will access that software on the network at any given time.

Adhering to copyright laws and vendor terms and conditions will protect all parties. Measures which financial institutions may employ to protect against

copyright violations include:

- Obtaining a site license that authorizes use of the software at all PC locations within the organization.

- Assuring that employees are were informed about the rules governing site licenses.

While these measures may help prevent copyright violations, the best control mechanism is having a strict corporate policy that is communicated and enforced by management and auditors. Management must have an uncompromising attitude regarding copyright violations. The security administrator should be responsible for enforcing and monitoring the policy. Users should understand that unauthorized copying and/or usage of software is both legally and ethically wrong and that this practice is unacceptable under corporate standards.

DATA SECURITY

Just as hardware has to be protected, access to software and data also has to be restricted. Software and data are valuable assets and considerable damage including financial loss could be incurred if they are lost, stolen, or compromised. Implementing and enforcing data security controls will protect the data and software resources or any information that is transmitted and stored against accidental or intentional disclosure to unauthorized persons or for unauthorized modification or destruction. The seven essentials of data security are:

- Data should be protected from fire, theft and other physical hazards.

- Data should be reconstructible to recover from destruction or loss (intentional or accidental).

- Data should be auditable for prompt detection of loss and accidental and intentional manipulation.

- Systems should be tamper proof to prohibit programmers and systems analysts from bypassing controls.

- Users must be identified before being granted access.

- Systems must be able to check that user actions are authorized.

- User actions should be monitored so that suspicious or unauthorized behavior can be investigated.

Deliberate or accidental security exposures present in all data processing environments may be heightened by certain features of automated systems. Examples of deliberate threats include:

- A trapdoor or window built into the system by a programmer.

- Dumping portions of memory to obtain sensitive information, codes, passwords, etc.

- Misuse of another person's authorized access code, password, etc.

- Obtaining access codes or other restricted data by obtaining copies of hard-copy output from trash cans, etc.

- Obtaining access codes or other restricted data by wiretapping.

Examples of accidental threats include:

- Faults in the data communication system leading to erroneous data in the data base.

- Hardware or software failures leading to a breakdown of a built-in security feature. For example, secret data – such as passwords – may be printed as part of a core dump during an abnormal termination or a recovery.

The accuracy and integrity of data as well as continued operations depend on establishing proper control procedures and guidelines for processing in user and data processing areas within the financial institution. To ensure that data is secure and operations are uninterrupted the following key elements of data security for all platforms (mainframe, minicomputer, LANs, and PCs) should be reviewed:

- Logical access security.
- Data integrity.
- Telecommunications security.

- Output distribution controls.
- Virus protection strategy.
- User education.
- Accountability.

LOGICAL ACCESS SECURITY AND CONTROLS

Logical access security prevents unauthorized users from connecting or gaining access to application and system resources before and after achieving physical connection to PCs, local area networks, minicomputer or mainframe systems. Logical access security includes logical access controls (user IDs and passwords) and programming security (systems software access).

Logical Access Controls

Logical access security objectives should include identification and authorization of users. The degree of control present within each computer system depends on how it is used. For example, PCs can be used as standalone systems or as access links to mainframes, minicomputers, or LANs. In addition, differentiation must be made between computers that can access classified information and those which only utilize nonclassified information.

Exposures within each type of usage should be determined through risk analysis conducted under the supervision of the security administrator. The rules that determine access to specific systems and information should be based on such risk analysis. Before users receive their log-on ID and password, the level of security access or rules must be defined by departmental management and forwarded to the security administrator for implementation. Levels of access or rules should be predetermined to ensure consistency between user types.

Computer capability may be limited by function. Depending on the function and the sensitivity of the application or data, protection may be implemented at the system data base, file, record, or field level. Various authorized actions include read, write, execute, and allocate. Thus, user access can be limited to those functions necessary to perform a specific job.

A user ID grants initial access, and a password authenticates the user's authorization to access the system. User IDs must be specific to one user since it will determine what a user can access and serve as an audit trail for transactions done by that user. The password must be held in strict confidence. Passwords should be changed periodically or whenever compromised. They may be of fixed or variable lengths. Passwords should be difficult to guess and must be adequately protected. Methods of protection include:

- Maintaining passwords in protected storage.
- Storing passwords in encrypted format.
- Print suppression, scrambling, or overprinting passwords when entered at the terminal.
- Printing decoys to camouflage the true password.
- Limiting the number of attempts for accessing the system, for example, after three failures, access is denied.

The security administrator is responsible for maintaining user IDs and passwords. Personnel departments should track all terminations accurately and notify the security administrator of such actions. Passwords and user IDs also should be revoked when users will be absent for extended periods. It is recommended that an individual other than the security administrator regularly review system logs and exception reports for access violations. This provides the necessary checks and balances for managing systems security. Logs serve as an effective control in any on-line system. Information contained in the logs should include:

- Unauthorized attempts to gain access to the system. Such attempts should be logged automatically by the system and a documented review of the exception report maintained by management. The system may be programmed to disconnect the offending terminal or PC from the network and to alert the responsible officer by displaying a message on the computer console or on a terminal display monitored by a security group.
- Attempts to gain information above the user's level of accessibility. These attempts also should

be logged automatically by the system. If a user continually attempts to access unauthorized information, the system should notify the responsible officer, who should investigate the reason.

- A detailed transaction file for each application. At a minimum, this file should contain information about the transaction and identification of the terminal and operator that initiated the transaction. A separate transaction file should be maintained for each accessible master file. As transactions are received from a terminal station, the date, time and sequence number are added to the file by the system. The expanded transactions are then copied onto a disk or tape. In some systems, the program acknowledges each transaction as it is received. If the system fails, the terminal operator should know the status of the current transaction at the time of failure. Reconstruction after a system failure requires a strict control procedure to limit errors. The transaction log may be used, if necessary, to reconstruct the master file by posting the entries in the transaction log to the backup master file. Thus, providing a detailed transaction file not only aids security, but also can be used to recovery in the event of an outage.

- Changes to operating system parameters, security tables, and network parameters.

Third-party security software packages for all platforms (mainframes, minicomputers, PCs, and LANs) can be utilized to prevent users from unauthorized access to the computer system itself as well as applications and data. While major strides have been made over the past few years, the LAN environment still lacks the mature industry standard security packages currently found on the mainframe.

Built in security controls also are contained in certain database management systems such as Oracle, SQL Server, and DB2. Finally, security restrictions may be programmed into an application to prevent users from unauthorized access to highly confidential information.

In addition to user IDs and passwords, logical access protection may be as simple as removing storage media (e.g., diskettes, tapes, removable hard drives, etc.) and keeping it in a secure location. Other controls include automatic log-off, time of day controls, keyboard locks, and data/file encryption.

Various types of automatic log-off mechanisms exist on mainframes, minicomputers, and PCs. In some mainframe environments the security software will automatically log an individual out of the system if no processing or keyboard action has occurred over a brief period of time (e.g., 10 minutes). With PC-based security, the software does not typically log the user off after a designated timeframe, but suspends operations. The screen or monitor will blacken or shut-off, but the user stays at the same location within the application or system. The individual only needs to type in password to resume functionality at the point of suspension.

Terminals and/or PCs used as standalones, terminal emulators, or networking devices utilize the security software on the desired platform for further controls after initial access has been granted. Once the user logs onto the system, different methods are utilized to provide control such as user profile and authorization tables. User profiles are unique to each user and extend to programs, data files, terminals or PCs, time periods of access, executable transactions and commands. Authorization tables involve classifying users into various groups with associated access levels. Software may be available, however, that enables users to circumvent system security controls. For that matter, any person knowledgeable in programming also may be able to circumvent these controls. As a precaution, files containing user IDs, passwords, and log-on sequences should be assigned the highest level of security, permitting only limited access.

While user IDs and passwords protect against unauthorized access, they do not protect against unauthorized disclosures. Computers that are part of a network need further protection because they transmit data to other terminals or PCs (standalone and networked) as well as to mainframe or minicomputers. During transmission, all nodes can read traffic on the network, thus potentially compromising data. Telecommunications security, such as data encryption, is required to assure data integrity, confidentiality, and system availability.

While encryption is required to ensure the privacy of data during transmission, it also can be used to

protect data files when other security mechanisms are unavailable, such as passwords or physical access protection. In addition, if the files are highly confidential, encryption may be used with these controls. A unique cryptographic key is used for each data file. The key used to encrypt the data is provided by the system or user. The encrypted data is enciphered before it is stored so that it becomes unusable to anyone except the person who holds the encryption key. In communication encryption, a transmitted file is decrypted at its destination, that is data is not encrypted when stored. In contrast, a data file remains encrypted until it's used again by the individual who has the key. Once a file is encrypted, the encryption key must be safeguarded against unauthorized access or loss.

PROGRAM SECURITY

Strict security should be maintained over access to and use of computer programs. Procedures should be in effect to restrict unauthorized access to:

- Application programs.
- Operating systems programs.
- Data files.
- Documentation.
- Computer equipment.

In addition, periodic supervisory review of activity logs, time records, reports, and console sheets should be required. Software programs may be used to flag exceptions. Many systems offer additional techniques to ensure program security. These advanced systems have the capability to protect libraries, produce system activity logs, and restrict operator access to unauthorized functions.

Systems utility programs are valuable tools when used during program debugging, file maintenance, cataloging, or even daily operations of the overall computer environment. However, certain programs can be used to alter storage, data files, and object code; enter the supervisor state; and catalog, purge and rename programs. System utilities also have capabilities to alter or delete programs or data. Most computer manufacturers supply these programs as part of the operating system. Commonly encountered programs include:

- IBM systems – DITTO, DEBE, IMASZAP (Superzap), IEBGENER, IEBRENAM, MSHP, IEBUPDAT, DFU, PDM, RLU, SDA, SEU, Windowtool/400, WFU, POP, RPGC, and Query/400.

- Unisys systems – Cande, Patch, Dumpall, and file copy.

- NCR systems – TRXFIX, FIX, $EDIT, and $CLEDIT.

Programs like these should be controlled to prevent unauthorized use.

Unauthorized use of system utility programs can be controlled in several ways. These controls, however, will not be effective if they unnecessarily impede operations. System utilities can be controlled by:

- Installing a password system on all program libraries/directories, including the system utility library/directory. If password protection is used, measures must be taken to control access to the passwords. Passwords should be changed periodically.

- Using automated library systems. Several automated library systems that provide program security are available from equipment manufacturers and software vendors. Such programs restrict access to the program library/directory. They can produce daily reports identifying each program that was accessed and any program changes that were made.

Even the most sophisticated security system will fail if management does not establish, implement and maintain adequate internal and operating controls. Standards and procedures for all aspects of program development, processing, and maintenance are necessary. These must identify control responsibilities and processes for documentation, review and approval of various programming activities. Supervision of these functions is imperative for establishing and maintaining program integrity. See Chapter 12 for additional information on program security.

DATA INTEGRITY

Financial institutions cannot exist without reliable data. Audit procedures must be established to ensure the accuracy and integrity of data. In addition to strong physical and logical access security, input and processing controls which consists of value, range, consistency, and reasonableness checks will improve data quality as well as processing efficiency. Program and system software control mechanisms are needed to protect the integrity of the applications, ensure valid data is entered into the system, and notify the user and appropriate personnel when erroneous data has been submitted into the system. Finally, to ensure data integrity on all systems, duties should be segregated. For more information on this topic, see the 1996 *Handbook* section titled "MIS Review" (Chapter 11).

Input and Processing Controls

Manually entering data into computers via terminals or PCs is a common practice. Most widely used are key-to-disk or key-to-tape entry systems. Data edit procedures can significantly reduce manual entry errors during input. In addition, edits can be built into programs and applications to ensure that data are being processed are valid. System software can provide a high degree of input and processing error controls.

A control mechanism to prevent unauthorized data alterations is to prohibit programmers and end-users from utilizing live data files for testing, training, and demonstrations. Program testing data or duplicate copies of actual data should be used for that purpose. In some organizations, it is common to find a centralized group responsible for providing such data and specifying test cases to run. In addition, a risk to the confidentiality and accuracy of customer data exists if data center computer devices can be used to make entries to live files or to retrieve sensitive information not required by IS operations personnel in their performance of assigned duties. Strict access and authorization controls should exist for such computers.

The proliferation of PCs and distributed processing (e.g., LANs) has resulted in data being stored and processed on multiple platforms. This causes a number of potential problems, such as the duplication of data and varying complex security access systems.

In a distributed environment, data integrity is a greater risk and concern than with centralized mainframe systems. There are more opportunities to transform the data as it moves through the various systems. The automation technology is such that data from different areas of an institution is being funneled from several different, if not independent, systems which may be accurate. As an example, a report provided to the board of directors can be consolidated from 20 separate reports. Some of the data is generated by individual PCs; some connected to LANs, and others connected to the mainframe.

Another data integrity concern for network systems (e.g., mainframe, LANs, etc.) is where multiple users have access to shared data files and two or more users want to access and update the same files or records simultaneously. Software locking mechanisms can be utilized to prevent concurrent access. Several locking options include manual file locking and automatic record/file locking. Manual file locking allows the user to request that a lock be placed on the data that is to be used before to accessing the file or record. Automatic record/file mechanisms programmatically prohibits others from using data once the file/record has been accessed.

As data is transferred either manually or in an automated format between environments, the exposure to inaccuracies and/or loss of information is enhanced. Security mechanisms, such as logical access controls, automatic and/or manual cross verification of data, and programmatic and system software error controls will minimize the potential of data integrity risks.

Due to technologies that continuously change, increased end-user proficiencies, and unfamiliarity of security controls and processes within user areas, the integrity of information being generated by data processing systems for use by management, the board of directors, and the regulators should receive a sufficient level of review. Emphasis should be placed on the internal and/or external audit processes for reviewing and ensuring data integrity. Greater emphasis should be placed on evaluating sources and uses of data, critical computer applications, and the audit coverage afforded the integrity of critical information. If information integrity is not audited, then someone should sample and test key data and reports for accuracy on a periodic basis. As the

number of systems proliferate, so may errors and the potential for misleading if not fraudulent reporting. Thus, the decision-making processes resulting from critical information produced within the information systems environments may lead the organization to unsafe and/or unsound practices.

Output Controls

Whether displayed on a terminal monitor or on a report, visual access to sensitive information must be controlled. Within a financial institution or data processing center, there is a significant amount of information which is either printed and maintained in hardcopy format, stored and distributed via removable media (hard and floppy disks, tapes, etc.) or displayed visibly on CRT terminals and similar devices.

Written procedures for using system report generators need to be in place since users could query information they would otherwise have no process authority for. Additionally, any routine, pre-structured query instructions should be reviewed before authorization is given for their use and access to the instructions needs to be limited to ensure their integrity.

Sensitive data that is printed outside the data center or central computer room must require a specific action before the data is printed. Classified data must never be printed automatically to a remote printer. Once the report/data is released to the remote printer, the user must secure the output immediately.

Sensitive reports never should be left unattended by a copy or facsimile machine on an individual's desk. Classified information must be secured in a locked desk or cabinet to prevent the possibility of theft, unauthorized disclosure, or modification. Procedures must be developed for disposal of confidential data. For example, shredding machines could be available to destroy hardcopy reports. A degauser (magnet) can eliminate or destroy hard and floppy disks and tapes that contain confidential data.

Segregation of Duties

Segregation of duties is critical to the accuracy and integrity of data on any platform (mainframe, minicomputer, LAN, and PC). Security control measures must include the separation of duties for all computer operations. The separation of duties is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud only can be committed through collusion. It also is a detective safeguard, that is, the more people who are involved in processing, the greater the probability that fraud will be detected.

The following are examples of separation of duties:

- Require input transactions to be reviewed foraccuracy and legitimacy by someone who has not been involved in their preparation.

- Require adjustments and corrections of master records to be reviewed and approved by someone other than the person who approves routine transactions.

- Separate the functions which relate to the preparation and approval of input and those which relate to the distribution and reconcilement of output.

- The information processing function should be independent of the user departments for which it processes information. Information processing personnel must be prohibited from initiating or authorizing any changes to applications, system software, master records, or other types of information stored on the system other than those required to effect recovery from processing failures

The PC user often performs all of the following duties: programming, testing, documentation, computer operation, input preparation, and reconcilements. In a traditional mainframe environment, each of these functions is performed by different individuals. This provides a more secure system. Segregating duties in PC operations is difficult and not always feasible. Consequently, compensating controls such as strict supervision of the conformance to policies and procedures and frequent review of input, output, reconcilements, as well as any changes to system software and applications are necessary.

As PC users gain expertise in the system, they become familiar with its security limitations. This knowledge could be an enticement to fraud. As a

preventive measure, cross-training, and mandatory vacations are recommended to assist management to detect evidence of illicit activity. Cross-training increases backup efficiency by creating a pool of individuals who can take over when the employee assigned to a particular function is unavailable, or has left the employ of the financial institution.

Segregation of duties also is critical in a network environment. For example, the person who makes changes to an application should not be the person who authorizes the change. In addition, much like the mainframe system, production and testing environments for application development and maintenance should be separate. All production work would come to a halt, if a user who is programming an application using the production files crashes the system. Finally, thorough testing must be completed before implementing software or an application to ensure data integrity, and operational feasibility.

TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS

Telecommunications or data communications is accessing a network or computer system from a non-direct link or remote location through satellite, radio microwave, or telephone line transmissions. Unauthorized dial-in access to mainframe, minicomputers, and LANs is a serious threat today. Precautions or control mechanisms must be in place to prevent threats to the financial institutions systems, applications, and data. Telecommunication controls generally are supplied for terminals, files and for data transmission. Many techniques used to control data communications systems are discussed in the following paragraphs.

Telecommunications Access Controls

Computers (terminals and PCs) have become a more common means of communication for programmers, internal user departments and customers. Additionally, the use of PCs and other types of intelligent terminals is expanding rapidly as costs decrease and software becomes more flexible and menu-driven. Controlled access becomes increasingly complex due to expanded computer capabilities, geographic dispersal of terminals and use of various communications paths. Security not only must address physical restrictions to the computers, but must also provide system controls by function, operator, transaction and data type.

Software security features, which may be an integral part of the operating system, provide proper identification of the user, terminal and transactions and apply constraints on when the network may be used. These features may include:

- Identification and authentication checks;
- Automatic call-back procedures.
- Authorized activity or function tests.
- Time of day control locks.
- Automatic timed log-off.
- Access exception reporting.
- Security logs.
- Management intervention (turning modem on/off).
- Encryption algorithms.
- Automatic log on ID suspension when the number of attempts at accessing the system have reached a specified limit.

The identification and authentication feature is a fundamental control. The system should identify and verify the user, the type, and location of the hardware, the date and time, the transactions attempted or performed and their status, and the data resources accessed. Users may be identified through any combination of techniques that include a unique identification code (often referred to as a personal identification number (PIN), encoded cards, badges, encryption or verification keys, physical traits (voice or fingerprints, etc.), or passwords. Passwords are the most commonly used identification control and authentication tool.

Identification and authentication of physical computers is especially important. Terminals and PCs are connected to the system by modems, dataphones, or acoustical-couplers attached to public or leased lines. Some computers can be identified by two levels of special identification numbers which are encoded internally. The lower level identifies the terminal or PC. The higher level provides transmission of a security code that is installed in tamper-proof circuitry to protect against the interchanging of computers. These numbers can be verified automatically against a protected table of valid identifiers maintained by the system.

Another technique used to validate computers after a user has signed on, is the call-back method, where the system disconnects the terminal or PC and reconnects the line to a valid address. For dial-up systems, phone numbers should be adequately protected and changed periodically.

In certain situations, institutions will allow installation of PCs at employees' homes, with access to the mainframe or PC-based LAN via modems. Provisions for close supervision of home use of PCs should be implemented by the security administrator. Strict policies must be established to govern such use, including:

- Senior management approval.
- Screening employees who have this privilege.
- Establishing separation procedures which provide for the return of the computer and invalidation of logical access privileges when employees are terminated (voluntary or involuntary).
- Limiting employee activities performed via dial-up mode.
- Prescribing disciplinary actions for violations.

Regardless of the location of the remote computer, all users should be subject to the same data security measures as are those in-house. Once a user has passed the identification/authentication process, access should be allowed only to authorized systems, information, transactions, and commands.

The extent of telecommunications security in an organization varies and depends on risks and costs. In each instance, the comprehensiveness and effectiveness of existing controls should be determined by carefully assessing the system's security risk and the potential effect to the financial institution.

TRANSMISSION CONTROLS

Special controls must be in place to protect the confidentiality and accuracy of transmitted data. The reliability of transmitted data may be improved by using telecommunications controls such as:

- Parity checks.
- Message Authentication.
- Encryption.
- Error checking transmission protocols.

Although satellite and radio microwave transmissions are used, telephone lines are the most common method of linking the remote user with a central processor be it a mainframe, minicomputer, or LAN server. Since telephone lines are not maintained exclusively by the data center, physical and procedural controls should be reviewed to determine that the system is both reliable and secure from outside penetration.

Essentially, two types of telephone lines may be used in a teleprocessing system: dedicated private (or leased) lines and dial-up (or switched) lines. Dedicated lines are devoted 100 to the transmission of data between the host computer and the end-user device. The consistent quality of transmission and improved security afforded by dedicated lines make them preferable to dial-up lines. However, the versatility and low cost of dial-up lines make them useful in many instances such as low volume, infrequent communications, or as a backup means of transmission should dedicated lines become inoperable. Two types of dial-up lines can be used: regular public telephone communication lines and hybrid systems that use leased lines not specifically dedicated to a private user.

While communication line penetration is not easy, data communication systems are susceptible to exposure from line penetration or interception. The penetrate a teleprocessing system depend on the perpetrator's technical knowledge of data communications, the vulnerability and accessibility to equipment. A telecommunications system is vulnerable to penetration or message interception through several methods:

- Masquerading – Pretending to be an authorized user or repair person to gain access to the system. Access to user identification and authentication codes (if they are in use) would be necessary.
- Eavesdropping – Tapping or cutting in on telecommunications transmissions to monitor messages without interfering with them. Access to identifiable communications lines or links

would be necessary.

- Piggybacking – Monitoring transmitted messages to intercept, modify or replace and then retransmit to the host computer or user. Line access is required for piggybacking. In addition, a perpetrator would need a terminal capable of interfacing with the penetrated telecommunications system.

- Between lines – Inserting a compatible terminal into the communications channel. The system is accessed whenever the authorized user is signed on but inactive.

- Line grabbing – Inserting a compatible terminal into the telecommunications line. The perpetrator eavesdrops on the line until the authorized user signs-off. The sign-off message is intercepted and prevented from reaching the host system. The user is sent a false sign-off acceptance message, thereby giving the perpetrator free access to the system.

It is not possible to physically secure the communications lines, particularly when satellite or radio microwave links are used. However, the following methods may be utilized to reduce the penetration and transmission exposures inherent in these systems:

- Restricting access to documentation describing system design and development and listing the locations of telephone equipment and related teleprocessing communication lines. In view of the highly vulnerable and sensitive nature of communications equipment, all non-authorized personnel should be identified and supervised properly while in its general vicinity. Additionally, the specific telephone lines dedicated to on-line processing might be left unmarked or unidentified to hinder wiretapping or intentional sabotage. Codes for identifying all communications links could be used; their inventory should be kept in a secure area.

- Encrypting all passwords and vital data transmitted over the system. Encryption enables the transmission of data or messages in a format that discourages or prevents using data gained by unauthorized interception. There are two types of encryption:

  - Reversible encryption occurs when the sending unit transforms the clear text into cipher text and the receiving unit decrypts the cipher text back into the original clear text.

  - Irreversible encryption involves only the transformation of clear text into cipher text. There is no procedure to decrypt. This is useful, for example, for the internal storage of PIN's. (Encryption is generally used whenever the transmission of data requires that it be protected against unauthorized disclosure and undetected modification. Data encryption generally protects a transmission from interception and de-encryption by all but the most sophisticated interloper.)

- Using authentication checks on all transmitted messages. This would provide the receiving station with assurances of message validity. A code is inserted into each message based upon a sequential number, calculation or an algorithm tied to the last previously authenticated message.

- Using communications specialists to inspect telephone closets or install detection devices using limited terminal polling to determine the existence of wiretaps.

- Serially numbering each transaction received from a terminal or PC with a unique identifier. In some instances, the numbering process includes the date and time of day.

- Using automatic disconnects. Any terminal or PC inactive for a predetermined time period is disconnected automatically from the computer system.

- Using time-of-day controls where access is restricted to specific authorized times. Access at any other time would require supervisory approval.

Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are being transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. The former are used more often because error correcting codes are costly to implement and are unable to correct all errors.

Generally, error detection methods such as a check bit and redundant transmission are adequate.

Redundancy checking is a common error detection routine. A transmitted block of data containing one or more records or messages is checked for number of characters or patterns of bits contained in it. If the numbers or patterns do not conform with predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit it.

Check bits are often added to the transmitted data by the telecommunications control unit (TCU) and may be applied either horizontally or vertically. These checks are similar to the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check, and a parity check on all the equivalent bits is known as a horizontal, longitudinal, or row check. Use of both checks greatly improves the possibilities of detecting a transmission error, which may be missed when either of those checks are used alone. If only one parity check is used, a horizontal check is more effective, particularly when coupled with advanced character coding schemes.

The effectiveness of checking techniques in detecting data transmission distortions cannot be denied. If the capability for making these checks is not provided by the equipment manufacturer, they would be difficult to implement in-house. Therefore, error detecting techniques should be considered before making decisions regarding equipment purchases for teleprocessing networks.

COMPUTER VIRUSES

As networks have become commonplace and as PCs have proliferated, computer viruses have become a serious threat. Computer viruses have infected computer systems around the world and the threat is likely to continue.

Computer viruses are computer programs, unique in two respects: they can attach themselves to other computer programs, and they can replicate themselves and move to systems. These attributes are accomplished in such a way that the user may not realize the virus was even in the code until it becomes active. The virus may perform obvious actions (such as displaying a message) or may be more insidious by triggering entirely random actions (such as erasing parts of memory).

There are two types of computer virus, nondestructive and destructive. Nondestructive computer viruses usually take some kind of annoying action such as screen messages, screen blanking, changing monitor display colors, delaying execution of commands, etc. Destructive viruses, on the other hand, may partially or fully erase hard disk files and tables making them unusable or unrecoverable, do level formatting of disks, modify data files, suspend systems so they do not respond to keyboard entries, etc.

Computer viruses most often are encountered on networks and PCs. Due to the complexity of the operating system and the security on mainframe computers there have been very few cases of computer viruses on mainframe computers. However, with the increasing connectivity of computer networks and the trend toward more open systems, the threat of computer viruses is magnified. The fact that a virus can attach itself to code or messages that are transmitted over networks to unforeseen destinations, and that it can then replicate itself and begin the process all over again, means that an entire network, and the networks linked with it can be infected.

Virus Symptoms

Viruses can infect all PCs including those with DOS, UNIX, OS/2, and Macintosh operating systems. The following symptoms may indicate the presence of a computer virus:

- A program grows larger for no apparent reason.
- The number of bad sectors on hard disk suddenly increases.
- The appearance of icons changes inexplicably.
- The system freezes up or crashes.
- Available memory is filled up suddenly with trash, zeros, or other unexpected data making it unavailable.
- The hard disk accesses become more error prone (file not found messages).
- The disk drive light comes on when there is no known disk activity (saving a file, copying, etc.).
- The PC does not respond to the keyboard in a consistent manner.

Of course, many computer viruses let the victim know that they have indeed been a victim and either display a telltale message or quite visibly demonstrate that things are going astray. In such cases, there can be little doubt about virus infection. Other viruses wait for a predetermined event to occur such as a date. This is the case with the Friday the 13th virus and Michelangelo (March 3) birthday virus. If one of these is suspected, the system should be recovered with software from uninfected sources before the event or the computer date set ahead.

Controls

Viruses can infect a PC through public software (shareware) loaded from the floppy drive or through programs transmitted from public electronic bulletin boards. Therefore, one of the best ways to prevent computer viruses is not to allow them an entry into the PC.

Preventive controls are:

- Do not load computer programs from public electronic bulletin boards or other untrusted sources. If these must be used, load into an isolated computer until the programs can be adequately tested.
- Use diskless PCs if feasible.
- ALWAYS put write-protect tabs on original diskettes before loading into the computer for the first time. If the computer does not have a hard disk, always boot from a write-protected diskette.
- Viruses commonly attack the DOS COMMAND.COM file in the root directory. To protect it and other DOS software program files, make them READ ONLY by using the ATTRIB +R feature.
- Make backups on a regular basis, but be aware that even backups may be infected. Protect original disks and do not leave them in open areas.
- For networks, do not permit network users to access any outside bulletin boards (including the internet) without prior approval. Do not allow any transfer of executable programs over the network. This would also include connections from the internal network to the Internet.
- Virus scan all new or foreign diskettes before using on a PC, including newly purchased software.

Organizations should have a security policy which prohibits using untested or unlicensed software, loading software from bulletin boards, or using shareware that has not been validated. The policy also should prohibit copying of software and using personal software on the organization's PCs.

If computer viruses cannot be prevented, the next best line of defense are detective controls that detect the presence of a virus. There are a number of good antivirus software programs on the market which can detect the presence of various types of viruses. They can be run at the option of the user or be run automatically whenever the computer is powered up, the program can be executed by the AUTOEXEC.BAT file. The user should be cautioned that antivirus software should be periodically updated by the vendor in order to account for new viruses or new techniques.

Corrective controls are the final defense against computer viruses. Isolate any system that is suspect. Stop all processing on the system or network. The user should not attempt to replace infected programs and recover the systems. Special procedures should be predetermined and followed to isolate and recover from computer viruses.

There are special tools and utilities for recovery and restoring files (PC TOOLS, Norton Utilities, MacTools) without having to rebuild entirely from scratch. However, these should only be used by the expert user and not a novice to avoid even more damage. If in doubt, seek expert assistance.

Caution should be used before restoring from backup copies as they may also have the virus. There truly is no 100 percent safe method for virus protection, but vigilance and careful procedures will minimize the risk.